AMENDMENTS TO THE CLAIMS

Please amend claims 1, 3, 6, 9, 11-17, 19-26, and 28-42. Following is a complete listing of the claims pending in the application, as amended:

1. (Currently amended) A method of securing stored data on a computer system, the method comprising:

providing receiving one of several different password data to at the computer system;

transforming key data with one of the several different password data in a reversible fashion to produce encoded key data such that the one of the several different password data is required in order to perform a reverse transform and extract the key data from the encoded key data; and

storing the encoded key data such that the one of the several different password data and one of a plurality of user authorization processes, in combination, provide access to the key data,

wherein the key data is encoded with each of said the several different password data to provide different encoded key data for each user authorization process such that a combination of one of said the user authorization processes and a respective password data of the several different password data allows for retrieval and decoding of the key data, and

wherein the key data is for performing at least one of encrypting and decrypting the stored data on the computer system.

2. (Canceled)

3. (Currently amended) The method of claim 1, wherein each encoded key data is associated with one or more user authorization processes such that a combination of one or more user authorization processes and any of said the several different password data allows for retrieval and decoding.

4. (Previously presented) The method of claim 1, wherein the user authorization process is a biometric information verification process.

5. (Canceled)

6. (Currently amended) A method of securing stored data on a computer system, the method comprising:

~~providing a biometric information source and~~ comparing ~~the~~ a biometric information source against stored templates associated with the biometric information source and, ~~in dependence~~based upon a comparison result, pairing a biometric information source with a first individual identity;

~~providing~~ receiving one of several different password data associated with the first individual identity, the one of the several different password data being other than that stored on the computer system; and

retrieving encoded key data associated with the biometric information, and using the one of the several different password data for decoding the encoded key data,

wherein the key data is encoded with ~~said~~the several different password data to provide different encoded key data for each user authorization process such that a combination of user authorization by ~~said~~ the biometric information source in one of ~~said~~ the user authorization processes and a different one of the several different password data allows for retrieval and decoding of the same security data, and

wherein the key data is for performing at least one of encrypting and decrypting the stored data on the computer system.

7. (Canceled)

8. (Previously presented) The method of claim 6, wherein the decoded key data is for allowing access of the stored data to the identified individual.

9. (Currently amended) The method of claim 6, ~~wherein providing~~further comprising receiving the biometric information source at the computer system before comparing the biometric information source, and wherein receiving the biometric information source comprises imaging the biometric information source using a contact imager.

10. (Previously presented) The method of claim 9, wherein the contact imager is a fingerprint imager.

11. (Currently amended) The method of claim 6, wherein ~~providing~~ receiving ~~the~~ one of ~~the~~ several different password data associated with the first individual identity comprises ~~providing~~ receiving a password.

12. (Currently amended) The method of claim 6, wherein ~~providing~~ receiving ~~the~~ one of ~~the~~ several different password data associated with the first individual identity comprises ~~providing~~ receiving information stored on a smart card.

13. (Currently amended) A method of securing data, the method comprising:

~~providing~~ receiving a first information sample ~~to~~ at a computer system;

encoding one of several different password data in dependence upon the first information sample to produce key data, the key data for use in decoding stored encoded data;

~~providing~~ receiving at least one biometric information sample; and

securing the key data in dependence upon the at least one biometric information sample,

wherein the key data is encoded with ~~said~~ the several different password data to provide different encoded key data for each user authorization process such that a combination of user authorization using ~~said~~ the biometric information sample in one of ~~said~~ the user authorization processes and a different one of the several different password data allows for retrieval and decoding of the key data, and

wherein the key data is for performing at least one of encrypting and decrypting the stored data on the computer system.

14. (Currently amended) The method of claim 13, wherein ~~providing~~ receiving a first information sample ~~to~~at a computer system comprises hashing the first information sample to produce a first hash value.

15. (Currently amended) The method of claim 13, further comprising:

~~providing~~ receiving a second other information sample ~~to~~at the computer system;

hashing the second information sample to produce a second hash value;

encoding the one of the several different password data in dependence upon the second hash value to produce second key data; and

securing the second key data in dependence upon the at least one biometric information sample.

16. (Currently amended) The method of claim 13, wherein ~~providing~~ receiving the first information sample ~~to~~ at a computer system comprises ~~providing~~ receiving a password.

17. (Currently amended) The method of claim 13, wherein ~~providing~~ receiving the first information sample ~~to~~ at a computer system comprises ~~providing~~ receiving information stored on a smart card.

18. (Canceled)

19. (Currently amended) A method of securing data, comprising:

~~providing~~ receiving a first information sample ~~to~~ at a computer system;

~~providing~~ receiving at least one biometric information sample;

encoding the at least one biometric information sample using the first information sample;

encoding one of several different password data ~~in dependence~~based, at least in part, ~~upon~~ on the encoded biometric sample to produce key data; and

securing the key data ~~in dependence upon~~based, at least in part, on the at least one biometric information sample,

wherein the key data is encoded with ~~said~~ the several different password data to provide different encoded key data for each user authorization process such that a combination of user authorization using ~~said~~ the biometric information sample in one of ~~said~~ the user authorization processes and a different one of the several different password data allows for retrieval and decoding of the key data, and

wherein the key data is for performing at least one of encrypting and decrypting the stored data on the computer system.

20. (Currently amended) The method of claim 19, ~~comprising~~wherein:

~~providing~~ receiving a first information sample ~~to~~ at a computer system comprises receiving a first information sample for decoding the encoded biometric sample; and

wherein the method further comprises comparing the decoded biometric sample against stored templates associated with the biometric information source.

21. (Currently amended) The method of claim 19, wherein ~~providing~~ receiving a first information sample ~~to~~ at a computer system comprises hashing the first information sample to produce a first hash value.

22. (Currently amended) A computer system ~~that~~ for ~~secures~~ securing stored data, the computer system comprising:

an input device ~~that~~ configured to provides at least one of several different password data to the computer system;

a processing device ~~that~~ configured to encodes key data with ~~said~~ the several different password data in a reversible fashion to produce different encoded key data for each user authorization process such that respective

ones of the several different password data are required in order to perform a reverse transform and extract the key data from the encoded key data, wherein the processing device uses the key data for performing at least one of encrypting and decrypting the stored data on the computer system;

a memory device ~~that~~ configured to stores the encoded key data; and

a user authorization process ~~that~~ configured to retrieves the encoded key data from the memory device such that at least one of the several different password data and the user authorization process, in combination, provide access to the key data, wherein a combination of user authorization using said user authorization process and a different one of the several different password data allows for retrieval and decoding of the key data.

23. (Currently amended) The computer system ~~according to~~of claim 22, further comprising a plurality of user authorization processes, wherein each encoded key data is associated with one or more user authorization processes such that a combination of one or more user authorization processes and any of ~~said~~ the several different password data allows for retrieval and decoding of the key data.

24. (Currently amended) The computer system ~~according to~~of claim 22, wherein the user authorization process is a biometric information verification process.

25. (Currently amended) The computer system ~~according to~~of claim 22, wherein the one of the several different password data includes a password.

26. (Currently amended) A computer system ~~that~~ for ~~secures~~ securing stored data, the computer system comprising:

means for comparing a biometric information source against stored templates associated with the biometric information source and, in dependence upon a comparison result, pairing a biometric information source with a first individual identity;

an input device ~~that~~ configured to provides to the computer system a different password data for each user authorization process associated with the first individual identity, the password data being other than stored on the computer system;

means for retrieving encoded key data associated with the biometric information and for using the password data for decoding the encoded key data, wherein a combination of user authorization by ~~said~~ the biometric information source in one of ~~said~~ the user authorization processes and a different one of the different password data allows for retrieval and decoding of the same key data; and

means for performing at least one of encrypting and decrypting the stored data on the computer system using the decoded key data.

27. (Canceled)

28. (Currently amended) The computer system ~~according to~~of claim 26, wherein the decoded key data allows access to the stored data by the identified individual.

29. (Currently amended) The computer system ~~according to~~of claim 26, wherein the comparing means comprises a contact imager ~~that~~ configured to images the biometric information source.

30. (Currently amended) The computer system ~~according to~~of claim 29, wherein the contact imager is a fingerprint imager.

31. (Currently amended) The computer system ~~according to~~of claim 26, wherein at least one of ~~said~~ the different password data comprises a password.

32. (Currently amended) The computer system ~~according to~~of claim 26, wherein at least one of ~~said~~ the different password data is stored on a smart card.

33. (Currently amended) A computer system ~~that~~ for ~~secures~~ securing stored data, the computer system comprising:

an input device ~~that~~ configured to provide~~s~~ a first information sample to the computer system;

means for encoding a key data with different password data for each user authentication process in dependence upon the first information sample to produce first security data, the key data for use in decoding the stored data;

a biometric input device ~~that~~ configured to provide~~s~~ at least one biometric information sample;

means for securing the first security data in dependence upon at least one of the at least one biometric information sample in one of ~~said~~ the user authorization processes, wherein a combination of user authorization using ~~said~~ the biometric information sample and any of said different password keys allows for retrieval and decoding of the key data; and

means for performing at least one of encrypting and decrypting the stored data on the computer system using the decoded key data.

34. (Currently amended) The computer system ~~according to~~of claim 33, further comprising means for hashing the first information sample to produce a first hash value.

35. (Currently amended) The computer system ~~according to~~of claim 33, wherein the first information sample comprises a password.

36. (Currently amended) The computer system ~~according to~~of claim 33, wherein the first information sample is stored on a smart card.

37. (Currently amended) The computer system ~~according to~~ of claim 33, wherein the encoding means encrypts data using the key data.

38. (Currently amended) A computer system ~~that~~ for ~~secures~~ securing stored data, comprising:

an input device ~~that~~ configured to provides a first information sample to the computer system;

a biometric input device ~~that~~ configured to provides at least one biometric information sample to the computer system;

means for encoding the at least one biometric information sample using the first information sample and for encoding one of several different password data in dependence upon the encoded biometric sample to produce key data, the key data for use in decoding stored encoded data, wherein the key data is encoded with ~~said~~ the different password data for each user authorization process to provide different encoded key data such that a combination of user authorization using ~~said~~ the biometric information sample in one of ~~said~~ the user authorization processes and any of ~~said~~ the different password data allows for retrieval and decoding of the key data;

means for securing the key data in dependence upon at least one of the at least one biometric information sample; and

means for performing at least one of encrypting and decrypting the stored data on the computer system using the decoded key data.

39. (Currently amended) The computer system ~~according to~~of claim 38, further comprising:

means for decoding the encoded biometric sample using a first information sample provided by the input device; and

means for comparing the decoded biometric sample against stored templates associated with the biometric information source.

40. (Currently amended) A computer readable storage medium for securing stored data on a computer system, the computer readable storage medium having computer executable instructions stored thereon that, when executed, perform ~~the~~ a method, comprising:

~~providing one of several different password data to the computer system;~~

transforming key data with one of ~~the~~ several different password data from the computer system in a reversible fashion to produce encoded key data such that the one of the several different password data is required in order to perform a reverse transform and extract the key data from the encoded key data; and

storing the encoded key data such that the one of the several different password data and one of a plurality of user authorization processes, in combination, provide access to the key data,

wherein the key data is encoded with each of ~~said~~ the several different password data to provide different encoded key data for each user authorization process such that a combination of one of ~~said~~ the user authorization processes and a respective password data of the several different password data allows for retrieval and decoding of the key data, and

wherein the key data is for performing at least one of encrypting and decrypting the stored data on the computer system.

41. (Currently amended) The computer readable medium of claim 40, wherein each encoded key data is associated with one or more user authorization processes such that a combination of one or more user authorization processes and any of ~~said~~ the several different password data allows for retrieval and decoding.

42. (Currently amended) The computer readable medium of claim 40, wherein the user authorization process is a biometric information verification process.